DirectCertify

Unlock Your Potential, Certify Your Success

CompTIA

CAS-005 Exam

CompTIA SecurityX Certification Exam

Exam Latest Version: 13.2

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.directcertify.com/comptia/cas-005

Question 1. (Multi Select)

[Security Architecture]

After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.

• Exfiltration of intellectual property

• Unencrypted files

• Weak user passwords

Which of the following is the best way to mitigate these vulnerabilities? (Select two).

A: Implementing data loss prevention
B: Deploying file integrity monitoring
C: Restricting access to critical file services only
D: Deployingdirectory-based group policies
E: Enabling modem authentication that supports MFA
F: Implementing a version control system
G: Implementing a CMDB platform

Correct Answer: A, E

Explanation:

To mitigate the identified vulnerabilities, the followingsolutions are most appropriate:

A . Implementing data loss prevention (DLP): DLP solutions help prevent the unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.

E . Enabling modern authentication that supports Multi-Factor Authentication (MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.

Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:

B . Deploying file integrity monitoring helps detect changes to files but does not prevent data exfiltration or address weak passwords.

C . Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.

D . Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.

F . Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.

G . Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.

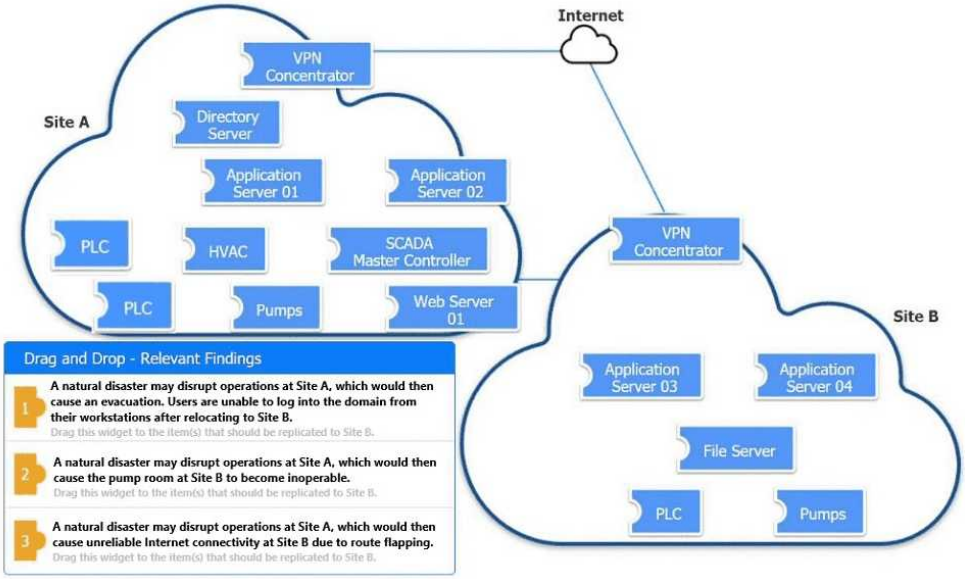
CompTIA Security+ Study Guide

NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

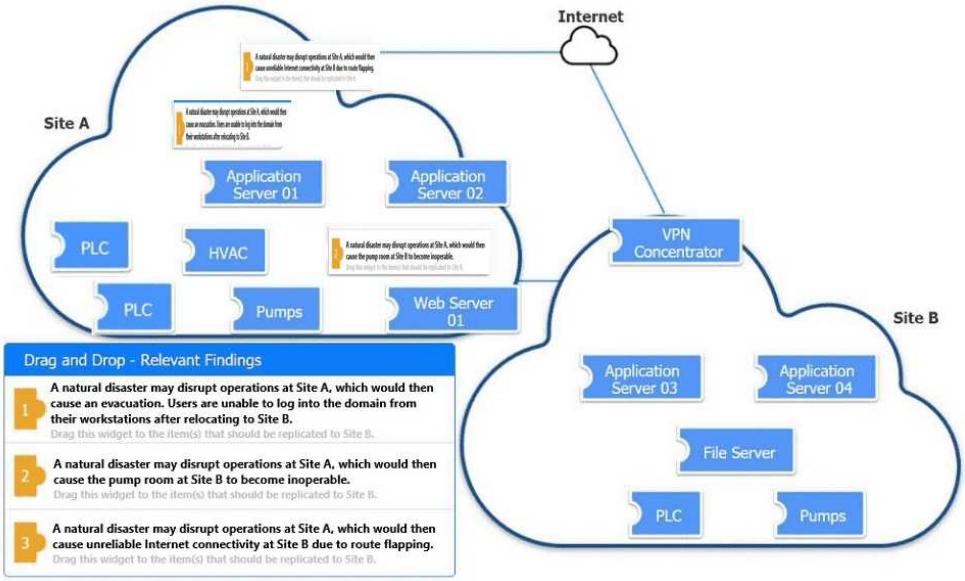
Question 2. (DRAGDROP)

[Security Architecture]



An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS Review the following scenarios and instructions. Match each relevant finding to the affected host. After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding. Each finding may be used more than once. If at any time you would like to bring back the initial state of the simul-ation, please click the Reset All button.

Correct Answer:



Question 3. (Single Select)

[Identity and Access Management (IAM)]

A security analyst is reviewing the following authentication logs:

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

Which of thefollowing should the analyst do first?

A: Disable User2's account
B: Disable User12's account
C: Disable User8's account
D: Disable User1's account

Correct Answer: D

Explanation:

Based on the provided authentication logs, we observe that User1's accountexperienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12/15). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Here’s a breakdown of why disabling User1's account is the appropriate first step:

Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts:

VM01 at 8:01:23 AM

VM08 at 8:01:23 AM

VM01 at 8:01:23 AM

VM08 at 8:01:23 AM

Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.

Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further failed attempts, which might lead to successful unauthorized access if not addressed.

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

CompTIA Security+ Certification Exam Objectives

NIST Special Publication 800-63B: Digital Identity Guidelines

By addressing User1's account first, we effectively mitigate the immediate threat of a brute-force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

Question 4. (Multi Select)

[Security Architecture]

After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.

• Exfiltration of intellectual property

• Unencrypted files

• Weak user passwords

Which of the following is the best way to mitigate these vulnerabilities? (Select two).

A: Implementing data loss prevention
B: Deploying file integrity monitoring
C: Restricting access to critical file services only
D: Deployingdirectory-based group policies
E: Enabling modem authentication that supports MFA
F: Implementing a version control system
G: Implementing a CMDB platform

Correct Answer: A, E

Explanation:

To mitigate the identified vulnerabilities, the followingsolutions are most appropriate:

A . Implementing data loss prevention (DLP): DLP solutions help prevent the unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.

E . Enabling modern authentication that supports Multi-Factor Authentication (MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.

Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:

B . Deploying file integrity monitoring helps detect changes to files but does not prevent data exfiltration or address weak passwords.

C . Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.

D . Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.

F . Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.

G . Implementing a CMDB platform (Configuration Management Database) helps manage IT

assets but does not address the specific security issues mentioned.

CompTIA Security+ Study Guide

NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

Question 5. (Single Select)

[Security Architecture]

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

• Unauthorized reading and modification of data and programs

• Bypassing application security mechanisms

• Privilege escalation

• interference with other processes

Which of the following is the most appropriate for the engineer to deploy?

A: SELinux
B: Privileged access management
C: Self-encrypting disks
D: NIPS

Correct Answer: A

Explanation:

The most appropriate solution for the systems engineer to deploy is SELinux (Security-Enhanced Linux). Here's why:

Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.

Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency.

Security Mechanisms: SELinux provides a robust framework to enforce security policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied.

Privilege Escalation and Process Interference: SELinux limits the ability of processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of privilege escalation attacks.

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

NSA's Guide to the Secure Configuration of Red Hat Enterprise Linux 5 (SELinux)

NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

DirectCertify

Unlock Your Potential, Certify Your Success

Full version is available at link below with affordable price.

https://www.directcertify.com/comptia/cas-005

30% Discount Coupon Code: LimitedTime2025